ICS 35.240.01
CCS L 67

DB33

浙 江 省 地 方 标 准

DB33/T 2488—2022

公共数据安全体系评估规范

Assessment specification for public data security systems

2022－04－26 发布　　2022－05－26 实施

浙江省市场监督管理局　　发 布

目　　次

前　言

本标准按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本标准的某些内容可能涉及专利。本标准的发布机构不承担识别专利的责任。

本标准由浙江省大数据发展管理局提出、归口并组织实施。

本标准起草单位：浙江省大数据发展中心、数字浙江技术运营有限公司、浙江省标准化研究院、联通数字科技有限公司、浙江省数据安全服务有限公司、杭州市数据资源管理局、宁波市大数据发展管理局、温州市大数据发展管理局、湖州市大数据发展管理局、嘉兴市政务服务和数据资源管理办公室、绍兴市大数据发展管理局、金华市大数据发展管理局、衢州市大数据发展管理局、舟山市大数据发展管理局、台州市大数据发展管理局、丽水市大数据发展管理局。

本标准主要起草人：金加和、王瑚、洪吉明、蓝宇娜、孟一丁、党铮铮、蒋纳成、赵程遥、毛远庆、张斌、杜永华、池邦芬、笪猛霄、陈焕、包自毅、张新丰、顾闻、徐振华、张晓玮、杜战、范东媛、费媛、叶春雷、孔俊、朱通、王沁怡、张伟伟、胡瑞玉、叶红叶、施筱玲、徐峰、蒋迪、甄理、俞巍滔、杜辉、孙茂阳、胡琼达、朱宝剑、叶茜茜、陈玮萍、屠勇刚、韩建良、徐李锐、毛勇增、张岳军、林国、王玲玲。

本标准为首次发布。

引　言

为保障一体化智能化公共数据平台和公共数据安全,建立健全数据安全防护能力评估指标,规范和指导各地各部门开展公共数据安全评估工作,推动全省公共数据安全管理工作可量化、可追溯、可评估,依据《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《浙江省公共数据条例》制定本标准。

本标准是公共数据安全体系相关系列标准之一。

与本标准的相关标准还包括:

——公共数据安全体系建设指南（DB33/T 2487—2022）;

——公共数据分类分级指南（DB33/T 2351—2021）。

公共数据安全体系评估规范

1 范围

本标准规范了公共数据安全体系评估总体要求、评估模型、评估项和评估流程等。

本标准适用于公共数据安全体系和能力评估，各级公共数据主管部门、公共管理和服务机构可参考执行。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本标准必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本标准；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 25069 信息安全技术 术语

GB/T 37973 信息安全技术 大数据安全管理指南

GB/T 37988 信息安全技术 数据安全能力成熟度模型

GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求

DB33/T 2350 数字化改革术语定义

DB33/T 2487 公共数据安全体系建设指南

3 术语和定义

GB/T 25069、GB/T 37973、GB/T 37988、GB/T 39477、DB33/T 2350和DB33/T 2487界定的以及下列术语和定义适用于本标准。

3.1

评估项 assessment item

与公共数据安全三个子体系对应，每一个子体系对应一个评估项，包括制度规范子体系评估项、技术防护子体系评估项和运行管理子体系评估项。

3.2

评估子项 assessment sub item

对应公共数据安全子体系各部分的建设内容，一个评估项包括若干个评估子项。

3.3

评估指标 assessment index

用以评估某一安全目标实现程度的数据安全相关活动和过程的最小单位，一个评估子项可基于评估内容，确定评估权重并赋予分值，定义若干个评估指标。

3.4

评估对象 assessment object

被评估的组织机构或部门，主要涉及相关配套制度文档、设备设施及人员等。

4 缩略语

下列缩略语适用于本标准。

AIT：评估项（Assessment Item）

AS：评估子项（Assessment Sub Item）

SUM：最终分值（Sum）

5 总体要求

5.1 科学性

评估项和评估方法的选取应能够体现公共数据安全体系的主要内容，反映公共数据安全保障面临的主要风险。

5.2 适宜性

评估项和评估方法的选取应结合本地区本部门实际情况，引导公共数据安全体系合理建设。

5.3 可度量性

评估项应具备可以获取的证明依据，并可以度量。

5.4 代表性

评估项应能较为全面地反映公共数据安全体系建设的总体水平。

5.5 持续性

应充分应用评估结果，促进公共数据安全体系的持续优化。

6 评估模型

6.1 总体架构

公共数据安全体系评估模型包括公共数据安全体系评估项、公共数据安全体系评估维度、公共数据安全体系评估方法。公共数据安全体系评估模型详见图1。

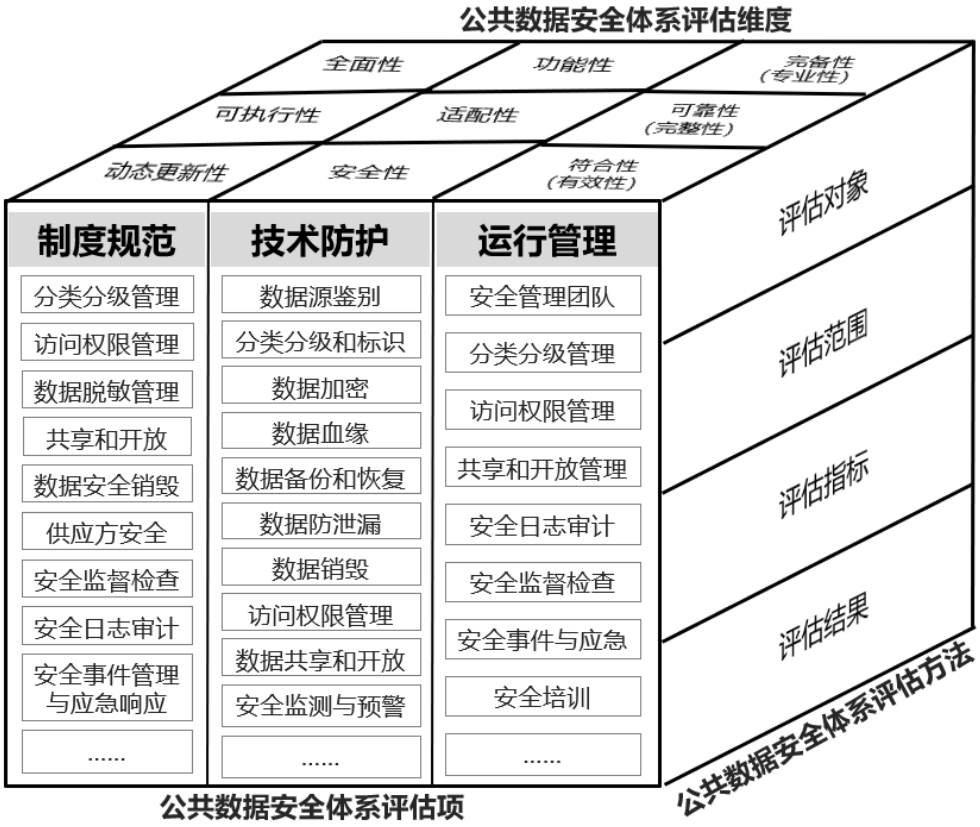

图1　公共数据安全体系评估模型

6.2　评估项

6.2.1　制度规范子体系评估项

制度规范子体系评估项可基于二级制度展开，主要包含的评估子项：

a）　分类分级管理制度；
b）　访问权限管理制度；
c）　数据脱敏管理制度；
d）　数据共享和开放安全管理制度；
e）　数据安全销毁管理制度；
f）　供应方安全管理制度；
g）　安全监督检查制度；
h）　安全日志审计制度；
i）　安全事件管理与应急响应制度等。

6.2.2　技术防护子体系评估项

技术防护子体系评估项主要包含的评估子项：

a）　数据源统一鉴别技术；
b）　敏感数据识别技术；
c）　数据分类分级标识技术；

d) 数据脱敏技术；
e) 数据加密技术；
f) 传输通道加密技术；
g) 数据血缘关系技术；
h) 数据备份和恢复技术；
i) 数据防泄漏技术；
j) 销毁数据识别技术；
k) 数据销毁技术；
l) 访问权限管理；
m) 数据共享和开放；
n) 安全监测与预警等。

6.2.3 运行管理子体系评估项

运行管理子体系评估项主要包含的评估子项：
a) 数据安全团队；
b) 数据分类分级运行管理机制；
c) 数据访问权限运行管理机制；
d) 数据共享和开放安全运行管理机制；
e) 安全日志审计机制；
f) 安全监督检查机制；
g) 安全事件应急响应机制；
h) 安全培训机制等。

6.3 评估维度

公共数据安全体系评估维度可根据公共数据安全体系评估项的特点设置，共分为3大类，包括：
a) 制度规范子体系评估维度，包括：
   1) 全面性：评估相关制度文件内容是否全面，是否已经包含了必要的组成要素；
   2) 可执行性：评估相关制度文件内容是否具备可落地执行性；
   3) 动态更新性：评估相关制度文件内容是否根据外部环境、政策变化、组织实际情况等进行了相应的调整。
b) 技术防护子体系评估维度，包括：
   1) 功能性：评估相关技术产品是否覆盖所有安全功能要求；
   2) 适用性：评估相关技术产品的安全功能和性能是否有效实现公共数据安全防护；
   3) 安全性：评估相关技术产品本身是否存在漏洞、配置错误（基线检查）、业务逻辑错误等安全问题。
c) 运行管理子体系-数据安全团队评估子项评估维度，包括：
   1) 完备性：评估该组织是否已安全评价指标配备团队人员；
   2) 专业性：评估相关人员是否有足够能力胜任职责范围内的工作，评估相关人员是否定期接受数据安全防护技能及法规培训等；
   3) 可靠性：评估相关人员是否有良好的职业操守，无相关不良记录情况。
d) 运行管理子体系-分类分级等其他运行管理机制的评估子项评估维度，包括：

1） 完整性：评估该运行管理机制是否包括完整的闭环运行管理环节；
2） 符合性：评估该运行管理机制是否已在该组织落地实施；
3） 有效性：评估该运行管理机制在该组织落实后，是否有效的实现公共数据安全防护预期效果。

7 制度规范子体系评估项

7.1 数据分类分级管理制度

公共数据分类分级管理相关制度评估子项内容主要包括：
——全面性：查验制度文件是否包括分类分级原则、要求、维度、方法、操作指南、工作流程以及类别和级别变更场景、变更申请审批流程及工作要求等；
——可执行性：充分考虑政策背景、行业技术发展情况、单位实际情况等，推演判断文件规定内容是否可在该组织落地实施；
——动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等，至少每年评估并修订相关制度文件，查验范围包括调研记录、修订记录等。

7.2 数据访问权限管理制度

公共数据访问权限管理相关制度评估子项内容主要包括：
——全面性：查验制度文件是否包括对公共数据载体和公共数据权限管理系统的账号权限安全管理职责分工和工作要求，公共数据访问账号权限分配、开通、使用、变更、重置、锁定、注销等的申请审批流程，对具备超级管理员权限或数据批量复制、处理、导出和删除等高风险操作权限的帐号的重点安全管理要求等；
——可执行性：充分考虑政策背景、行业技术发展情况、单位实际情况等，推演判断文件规定内容是否可在该组织落地实施；
——动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等，至少每年评估并修订相关制度文件，查验范围包括调研记录、修订记录等。

7.3 数据脱敏管理制度

公共数据安全脱敏管理相关制度评估子项内容主要包括：
——全面性：查验制度文件是否充分根据公共数据分类分级结果，是否包括公共数据脱敏规则、管理要求、技术要求和脱敏工作流程等；
——可执行性：充分考虑政策背景、行业技术发展情况、单位实际情况等，推演判断文件规定内容是否可在该组织落地实施；
——动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等，至少每年评估并修订相关制度文件，查验范围包括调研记录、修订记录等。

7.4 数据共享和开放安全管理制度

公共数据共享和开放安全管理相关制度评估子项内容主要包括：
——全面性：查验制度文件是否充分根据公共数据分类分级结果；查验制度文件是否包括差异化的公共数据共享和开放安全管理、技术要求、应用场景、工作流程和申请审批环节等；

——可执行性：充分考虑政策背景、行业技术发展情况、单位实际情况等，推演判断文件规定内容是否可在该组织落地实施；
——动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等，至少每年评估并修订相关制度文件，查验范围包括调研记录、修订记录等。

7.5 数据安全销毁管理制度

公共数据安全销毁管理相关制度评估子项内容主要包括：
——全面性：查验制度文件是否充分根据公共数据分类分级结果；查验制度文件是否包括公共数据销毁对象、销毁场景、销毁方式、销毁流程、销毁工作要求等；
——可执行性：充分考虑政策背景、行业技术发展情况、单位实际情况等，推演判断文件规定内容是否可在该组织落地实施；
——动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等，至少每年评估并修订相关制度文件，查验范围包括调研记录、修订记录等。

7.6 供应方安全管理制度

供应方安全管理相关制度评估子项内容主要包括：
——全面性：查验制度文件是否包括供应方及供应方人员的安全管理要求，涉及终端安全、网络安全、数据安全、保密管理等方面；查验制度文件是否包括供应方及供应方人员的岗位安全职责、安全考核要求和处罚措施；核查服务安全保护及保密协议是否明确了对供应方及供应方人员的数据保密范围、保密责任与义务、保密期限等；
——可执行性：充分考虑政策背景、行业技术发展情况、单位实际情况等，推演判断文件规定内容是否可在该组织落地实施；
——动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等，至少每年评估并修订相关制度文件，查验范围包括调研记录、修订记录等。

7.7 安全监督检查制度

公共数据监督检查相关制度评估子项内容主要包括：
——全面性：查验制度文件是否包括对公共数据安全体系建设现状的监督检查内容、方式、工作周期、工作流程等；
——可执行性：充分考虑政策背景、行业技术发展情况、单位实际情况等，推演判断文件规定内容是否可在该组织落地实施；
——动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等，至少每年评估并修订相关制度文件，查验范围包括调研记录、修订记录等。

7.8 安全日志审计制度

公共数据安全日志审计相关制度评估子项内容主要包括：
——全面性：查验制度文件是否包括安全审计日志的采集内容、采集方式、标准化要求、日志存储要求、审计策略和规则、异常预警及处置工作流程等；
——可执行性：充分考虑政策背景、行业技术发展情况、单位实际情况等，推演判断文件规定内容是否可在该组织落地实施；

——动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等，至少每年评估并修订相关制度文件，查验范围包括调研记录、修订记录等。

7.9 安全事件管理与应急响应制度

公共数据安全事件管理与应急响应相关制度评估子项内容主要包括：

——全面性：查验制度文件是否包括数据安全事件分类分级方法；核查制度文件是否充分结合数据安全事件分类分级结果；核查制度文件是否包括公共数据安全事件发现、上报、处置、溯源、总结等工作流程；核查制度文件是否包括数据安全应急预案编制及应急演练工作要求等；

——可执行性：充分考虑政策背景、行业技术发展情况、单位实际情况等，推演判断文件规定内容是否可在该组织落地实施；

——动态更新性：查验是否持续跟踪外部环境、政策变化、组织实际情况等，至少每年评估并修订相关制度文件，查验范围包括调研记录、修订记录等。

8 技术防护子体系评估项

8.1 数据源统一鉴别技术

数据源统一鉴别技术评估子项内容主要包括：

——功能性：检查该技术产品是否具备数据源身份统一鉴别、记录的功能，以及对数据真实性、有效性、规范性进行检验的功能；

——适用性：核查该技术产品是否有效防止非法数据源接入，实现防止虚假数据注入；核查该技术产品性能是否满足该组织业务高峰期需求等；

——安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。

8.2 敏感数据识别技术

敏感数据识别技术评估子项内容主要包括：

——功能性：检查该技术产品是否具备敏感数据识别功能；

——适用性：核查该技术产品是否可有效识别出敏感数据；核查该技术产品性能是否满足该组织业务高峰期需求等；

——安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。

8.3 数据分类分级标识技术

数据分类分级标识技术评估子项内容主要包括：

——功能性：检查该技术产品是否具备根据相关标准进行智能化分类分级的功能；检查该技术产品是否具备数据分类分级标识功能；检查该技术产品是否具有数据分类分级结果的输出接口，用于分类分级结果的应用；

——适用性：核查该技术产品是否可有效标识数据类别和级别；核查该技术产品性能是否满足该组织业务高峰期需求等；

——安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。

8.4 数据脱敏技术

公共数据脱敏技术评估子项内容主要包括：

——功能性：检查该技术产品是否可实现敏感数据脱敏功能；检查该技术产品是否可实现数据存储或使用脱敏功能（包含静态和动态脱敏）；检查该技术产品是否可根据不同场景配置不同的脱敏算法与规则等；

——适用性：核查是否已有效对规定场景数据进行静态或动态脱敏保护；核查该技术产品性能是否满足该组织业务高峰期需求等；

——安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。

8.5 数据加密技术

数据加密技术评估子项内容主要包括：

——功能性：检查该技术产品是否可实现敏感数据存储和传输加密功能；

——适用性：核查是否已有效对存储和传输的敏感数据实施加密保护；核查该技术产品性能是否满足该组织业务高峰期需求等；

——安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。

8.6 传输通道加密技术

传输通道加密技术评估子项内容主要包括：

——功能性：检查该技术产品是否可实现数据传输通道加密；

——适用性：核查是否已有效对数据传输通道实施加密保护；核查该技术产品性能是否满足该组织业务高峰期需求等；

——安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。

8.7 数据血缘关系技术

数据血缘关系技术评估子项内容主要包括：

——功能性：检查该技术产品是否具有追踪记录数据间的血缘关系的功能；检查该技术产品是否可根据数据血缘关系建立数据资产全景视图等；

——适用性：核查该技术产品是否可有效监控数据流转过程；核查该技术产品性能是否满足该组织业务高峰期需求等；

——安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。

8.8 数据备份和恢复技术

数据备份和恢复技术评估子项内容主要包括：

——功能性：检查该技术产品是否具备自动化数据备份的功能；检查该技术产品是否具备自动检验备份数据完整性的功能；检查该技术产品是否具备数据恢复的功能等；

——适用性：核查该技术产品在数据遭受破坏时，数据备份机制是否保存了恢复所需的数据，恢复机制是否能够根据备份数据有效恢复，保证业务受影响程度在可接受的范围内；核查该技术产品性能是否满足该组织业务高峰期需求等；

——安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。

8.9 数据防泄漏技术

数据防泄漏技术评估子项内容主要包括：

——功能性：检查该技术产品是否具备数据防泄漏功能，包括终端、网络和应用等；
——适用性：核查该技术产品是否有效实现了数据在终端、网络和应用等流转过程的防泄漏；核查该技术产品性能是否满足该组织业务高峰期需求等；
——安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。

8.10 销毁数据识别技术

销毁数据识别技术评估子项内容主要包括：
——功能性：检查该技术产品是否具备符合销毁场景数据的识别功能；
——适用性：核查该技术产品是否可有效识别符合数据销毁场景的数据；核查该技术产品性能是否满足该组织业务高峰期需求等；
——安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。

8.11 数据销毁技术

数据销毁技术评估子项内容主要包括：
——功能性：检查该技术产品是否具备多种数据销毁策略和技术手段等；
——适用性：核查该技术产品的销毁策略和手段是否可实现对数据的彻底销毁；核查该技术产品性能是否满足该组织业务高峰期需求等；
——安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。

8.12 访问权限管理技术

公共数据访问权限管理技术评估子项内容主要包括：
——功能性：检查该技术产品是否具备公共数据访问权限集中认证、统一访问入口等功能；检查该技术产品是否具备库、表、字段级别的访问控制功能；检查该技术产品是否与数据脱敏相关技术产品联动，实现动态脱敏等；
——适用性：核查该技术产品是否有效支撑该组织和角色职能需求，实现公共数据访问权限的有效管控；核查该技术产品性能是否满足该组织业务高峰期需求等；
——安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。

8.13 数据共享和开放安全技术

公共数据共享和开放的安全技术评估子项内容主要包括：
——功能性：检查该技术产品是否具备访问控制功能；检查该技术产品是否具备数据脱敏功能；核查该技术产品是否具备接口实时数据安全监测与异常告警功能；检查该技术产品是否具备数据追踪溯源功能，如数字水印标识等；
——适用性：核查该技术产品是否可有效支撑共享和开放数据的访问控制功能；核查该技术产品的数据脱敏能力是否可有效对共享和开放的数据实施脱敏，包括脱敏算法的类型、数量等；核查该技术产品是否可有效发现接口安全风险，并告警；核查该数据产品的溯源过程和结果是否可信，例如采用区块链技术等；核查该技术产品性能是否满足该组织业务高峰期需求等；
——安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。

8.14 安全监测与预警技术

公共数据安全监测与预警技术评估子项内容主要包括：

——功能性：检查该技术产品是否具备可配置化的量化指标的功能；检查该技术产品是否接入了全量重要系统的日志数据，并具备支撑威胁发现、识别、理解分析、风险预警和提供处置建议的能力等；
——适用性：核查该技术产品是否有效发现该组织数据安全风险，支撑数据安全体系建设规划；核查该技术产品性能是否满足该组织业务高峰期需求等；
——安全性：核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。

9 运行管理子体系评估项

9.1 数据安全管理团队

公共数据安全管理团队评估子项内容主要包括：
——完备性：检查是否设置公共数据安全管理团队，包括公共数据安全决策方、公共数据安全管理方、公共数据安全执行方、公共数据安全审计方等；检查是否明确公共数据安全管理团队的各方的职责分工；检查是否设置机构主要负责人为公共数据安全管理第一责任人；检查是否设置专职的公共数据安全管理负责人；检查是否明确公共数据安全管理第一责任人和负责人的工作职责等；
——专业性：查验公共数据安全管理负责人是否具备数据安全专业知识和履职能力，包括具备 CISP 等安全专业证书；查验公共数据安全管理负责人是否接受安全技能培训和考核；查验单位是否为公共数据安全管理负责人提供必备的人力支持和技术支持。查验该团队成员专业人员安全技术能力及安全专业证书覆盖程度，确保可胜任职责范围的工作；
——可靠性：查验该团队安全管理负责人和成员的背景、履历等情况。

9.2 数据分类分级管理机制

公共数据分类分级管理机制评估子项内容主要包括：
——完整性：查验该工作机制是否与数据资源目录机制协同；查验该工作机制是否建立维护了数据资产全景视图；查验该工作机制是否实现分类分级工作实施、工作结果反馈、分类分级机制优化的闭环管理等；
——符合性：查验分类分级工作实施、数据资源目录同步、分级结果反馈、分类分级机制优化等工作过程文件和记录；
——有效性：检查分类分级工作实施、数据资源目录同步、分级结果反馈、分类分级机制优化等工作结果文件和记录。

9.3 数据访问权限管理机制

公共数据访问权限管理机制评估子项内容主要包括：
——完整性：查验该工作机制是否包括公共数据访问权限的分配、开通、使用、变更、重置、注销等的申请审批、实施、以及定期核查等；查验该工作机制是否建立维护了统一的公共数据访问权限清单；
——符合性：查验公共数据访问账号权限分配、开通、使用、变更、重置、注销等的申请审批、实施、定期核查等工作过程文件和记录；
——有效性：检查公共数据访问账号权限分配、开通、使用、变更、重置、注销等的申请审批、实施、定期核查等工作结果文件和记录。

9.4 数据共享和开放安全管理机制

公共数据共享和开放安全管理机制评估子项内容主要包括：

——完整性：查验该工作机制是否包括公共数据共享和开放的申请审批，接口上线前和上线后的安全检查、敏感数据实时监测告警处置等；

——符合性：查验公共数据共享和开放的申请审批，接口上线前和上线后的安全检查、敏感数据实时监测告警处置等工作过程文件和记录；

——有效性：检查公共数据共享和开放的申请审批，共享和开放接口安全检查及整改、敏感数据实时监测告警处置及整改等工作结果文件和记录。

9.5 安全日志审计机制

公共数据安全日志审计机制评估子项内容主要包括：

——完整性：查验该工作机制是否包括违规行为告警的核实、分析、处置和整改等环节；

——符合性：查验违规行为告警的核实、分析、处置和整改等工作过程文件和记录；

——有效性：检查违规行为告警的核实、分析、处置和整改等工作的结果文件。

9.6 安全监督检查机制

公共数据安全监督检查机制评估子项内容主要包括：

——完整性：查验该工作机制是否包括安全监督检查工作实施、工作总结，问题整改、整改效果验证等环节；

——符合性：查验安全监督检查工作实施、工作总结，问题整改、整改效果验证等工作过程文件和记录；

——有效性：检查安全监督检查工作实施、工作总结，问题整改、整改效果验证等工作结果文件和记录。

9.7 安全事件应急响应机制

公共数据安全事件应急响应机制评估子项内容主要包括：

——完整性：查验该工作机制是否包括应急演练规划、实施、总结以及应急演练报告编制、应急预案优化等环节；

——符合性：查验应急演练规划、实施、总结以及应急演练报告编制、应急预案优化等工作过程文件和记录；

——有效性：检查应急演练规划、实施、总结以及应急演练报告编制、应急预案优化等工作结果文件和记录；检查安全事件发生时，应急响应工作记录和结果文件。

9.8 安全培训机制

公共数据安全培训机制评估子项内容主要包括：

——完整性：查验该工作机制是否包括培训计划制定、工作实施、效果考核、计划优化调整等环节；

——符合性：查验培训计划制定、工作实施、效果考核、计划优化调整等工作过程文件和记录；

——有效性：检查培训计划制定、工作实施、效果考核、计划优化调整等工作结果文件和记录。

10 评估流程

10.1 基本流程

公共数据安全体系评估流程应依据评估对象及评估目标，按照确定评估范围、组建评估团队、制定评估方案、实施评估和报告编制5个步骤实施，评估工作过程可参考图2。

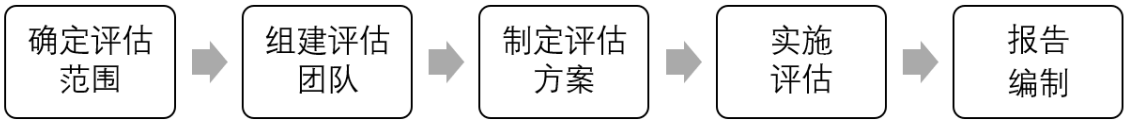

图2 评估工作过程示意图

10.2 确定评估范围

首先应明确评估范围，包括被评估方涉及评估的系统、应用、网络、终端以及相关部门和人员等。

10.3 组建评估团队

评估团队应由评估人员和被评估单位相关人员组成，可根据单位实际情况及评估范围，聘请相关专业机构或专家参与评估工作。被评估单位相关人员宜包括：

——公共数据安全管理人员；

——公共数据平台运维人员；

——公共数据相关基础设施（政务云、网络、终端等）运维人员；

——公共数据重点应用部门相关人员等。

10.4 制定评估方案

应制定评估方案。评估团队根据评估对象实际情况，确定评估场地、评估时间。依据评估范围选取对应的评估项（含子项）和评估维度，制定评估指标（取定评估权重和赋分规则可参考附录B），通过资料查询、人员访谈、问卷调查、功能演示和技术检测等评估方式，形成书面评估方案。评估方案主要包括:

a) 评估对象：被评估的组织机构或部门；
b) 评估范围：被评估方涉及评估的系统、应用、网络、终端以及相关部门和人员等；
c) 评估团队：评估人员和被评估单位涉及到的人员；
d) 评估场地：评估团队开展评估活动的地点；
e) 评估时间：评估起止时间；
f) 评估指标：评估子项内容、评估权重、赋分（参见附录 A）；
g) 评估方式（参见附录 B）：根据评估指标，确定主要评估方式。

10.5 实施评估

实施评估主要包括以下步骤：

a) 评估团队按照评估方案实施评估，收集并整理相关证明材料，初步研判各评估指标符合情况并记录评估过程信息；

b） 评估团队根据评估过程记录及证明材料，组织召开会议，与被评估单位确认研判结果，形成各评估指标得分；

c） 根据评估指标得分，计算评估子项分值。

计算方法可参见附录C。

10.6 报告编制

评估结果以报告形式展现，评估报告内容主要包括：

a） 评估对象；

b） 评估范围；

c） 评估团队；

d） 评估场地；

e） 评估时间；

f） 评估方式；

g） 评估指标及分值；

h） 评估过程记录及关键证明材料；

i） 安全风险；

j） 评估结论；

k） 整改建议、计划及已整改情况等。

评估工作案例可参见附录D。

附 录 A
（资料性）
公共数据安全体系评估指标定义示例

A.1 评估指标由评估子项内容、评估权重及赋分构成。

A.2 根据评估子项在该组织数据安全体系中的重要性设置该评估子项的权重值，权重值一般为 1-10 的整数。

A.3 所有高风险项应全部满足，出现一个及以上未满足高风险项且不进行整改的，公共数据安全体系评估结果暂缓出具。

A.4 公共数据安全体系评估指标定义示例见表 A.1。

表A.1 公共数据安全体系评估指标定义示例

序号	评估项(AIT)	评估子项（AS）	评估权重	赋分规则
1	制度规范子体系评估项（AIT_1）	数据分类分级管理制度（AIT_1-AS_1）	6	**全面性：**查验制度文件是否包括分类分级原则、要求、维度、方法、操作指南、工作流程以及类别和级别变更场景、变更申请审批流程及工作要求等。（全部满足得5分）
2				**可执行性：**判断文件规定内容是否可在该组织落地实施。（全部满足得3分）
3				**动态更新性：**查验是否持续跟踪外部环境、政策变化、组织实际情况等。（全部满足得2分）
4		数据访问权限管理制度（AIT_1-AS_2）	7	**全面性：**查验制度文件是否包括对公共数据载体和公共数据权限管理系统的账号权限安全管理职责分工和工作要求等。（全部满足得5分）
5				**可执行性：**判断文件规定内容是否可在该组织落地实施。（全部满足得3分）
6				**动态更新性：**查验是否持续跟踪外部环境、政策变化、组织实际情况等。（全部满足得2分）
7		数据脱敏管理制度（AIT_1-AS_3）	7	**全面性：**查验制度文件是否充分根据公共数据分类分级结果，是否包括公共数据脱敏规则、管理要求等。（全部满足得5分）
8				**可执行性：**判断文件规定内容是否可在该组织落地实施。（全部满足得3分）
9				**动态更新性：**查验是否持续跟踪外部环境、政策变化、组织实际情况等。（全部满足得2分）
10				**全面性：**查验制度文件是否充分根据公共数据分类分级结果，进行差异化的公共数据共享和开放安全管理、技术要求、应用场景、工作流程和申请审批环节等。（全部满足得5分）

表A.1　公共数据安全体系评估指标定义示例（续）

序号	评估项(AIT)	评估子项（AS）	评估权重	赋分规则
11	制度规范子体系评估项（AIT_1）	数据共享和开放安全管理制度（AIT_1-AS_4）	7	**可执行性：**判断文件规定内容是否可在该组织落地实施。（全部满足得3分）
12				**动态更新性：**查验是否持续跟踪外部环境、政策变化、组织实际情况等。（全部满足得2分）
13		数据安全销毁管理制度（AIT_1-AS_5）	5	**全面性：**查验制度文件是否充分根据公共数据分类分级结果，进行公共数据销毁对象、销毁场景、销毁方式、销毁流程、销毁工作要求等。（全部满足得5分）
14				**可执行性：**判断文件规定内容是否可在该组织落地实施。（全部满足得3分）
15				**动态更新性：**查验是否持续跟踪外部环境、政策变化、组织实际情况等。（全部满足得2分）
16		供应方安全管理制度（AIT_1-AS_6）	8	**全面性：**查验制度文件是否包括供应方及其人员的安全管理要求、供应方及其人员的岗位安全职责、安全考核要求和处罚措施、明确了对供应方及其人员的数据保密范围、保密责任与义务、保密期限等。（全部满足得5分）
17				**可执行性：**判断文件规定内容是否可在该组织落地实施。（全部满足得3分）
18				**动态更新性：**查验是否持续跟踪外部环境、政策变化、组织实际情况等。（全部满足得2分）
19		安全监督检查制度（AIT_1-AS_7）	5	**全面性：**查验制度文件是否包括对公共数据安全管理现状的监督检查内容、方式、工作周期、工作流程等。（全部满足得5分）
20				**可执行性：**判断文件规定内容是否可在该组织落地实施。（全部满足得3分）
21				**动态更新性：**查验是否持续跟踪外部环境、政策变化、组织实际情况等。（全部满足得2分）
22		安全日志审计制度（AIT_1-AS_8）	7	**全面性：**查验制度文件是否包括安全审计日志的采集内容、采集方式、标准化要求、日志存储要求、审计策略和规则、异常预警及处置工作流程等。（全部满足得5分）
23				**可执行性：**判断文件规定内容是否可在该组织落地实施。（全部满足得3分）
24				**动态更新性：**查验是否持续跟踪外部环境、政策变化、组织实际情况等。（全部满足得2分）
25		安全事件管理与应急响应制度（AIT_1-AS_9）	8	**全面性：**查验制度文件是否包括数据安全事件分类分级方法、公共数据安全事件发现、上报、处置、溯源、总结等工作流程、数据安全应急预案编制及应急演练工作要求等。（全部满足得5分）

表A.1　公共数据安全体系评估指标定义示例（续）

序号	评估项(AIT)	评估子项（AS）	评估权重	赋分规则
26	制度规范子体系评估项（AIT_1）	安全事件管理与应急响应制度（AIT_1-AS_9）	8	**可执行性：**判断文件规定内容是否可在该组织落地实施。（全部满足得3分）
27				**动态更新性：**查验是否持续跟踪外部环境、政策变化、组织实际情况等。（全部满足得2分）
28	技术防护子体系（AIT_2）	数据源统一鉴别技术(AIT_2-AS_{10})	4	**功能性：**检查该技术产品是否具备数据源身份统一鉴别、记录的功能，以及对数据真实性、有效性、规范性进行检验的功能。（全部满足得4分）
29				**适用性：**1.核查该技术产品是否有效。（全部满足得2分）2.核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
30				**安全性：**核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
31		敏感数据识别技术(AIT_2-AS_{11})	8	**功能性：**检查该技术产品是否具备敏感数据识别功能。（全部满足得4分）
32				**适用性：**1.核查该技术产品是否具备有效识别出敏感数据的功能。（全部满足得2分）2.核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
33				**安全性：**核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
34		数据分类分级标识技术(AIT_2-AS_{12})	8	**功能性：**检查该技术产品是否具备数据分类分级标识功能，以及具备对外同步接口等。（全部满足得4分）
35				**适用性：**1.核查该技术产品是否具备有效标识数据类别和级别的功能。（全部满足得2分）2.核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
36				**安全性：**核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
37		数据脱敏技术（AIT_2-AS_{13}）	8	**功能性：**检查该技术产品是否具备实现敏感数据脱敏功能，是否可实现数据存储或使用脱敏功能（包含静态和动态脱敏）。（全部满足得4分）
38				**适用性：**1.核查是否具备有效对存储或使用的数据进行静态或动态脱敏保护的功能。（全部满足得2分）2.核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
39				**安全性：**核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）

表A.1　公共数据安全体系评估指标定义示例（续）

序号	评估项(AIT)	评估子项（AS）	评估权重	赋分规则
40	技术防护子体系（AIT_2）	数据加密技术（AIT_2-AS_{14}）	5	**功能性：**检查该技术产品是否具备实现敏感数据存储加密、传输加密等功能。（全部满足得4分）
41				**适用性：**1. 核查是否已有效对存储和传输的敏感数据实施加密保护。（全部满足得2分）2.核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
42				**安全性：**核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
43		传输通道加密技术（AIT_2-AS_{15}）	6	**功能性：**检查该技术产品是否可实现数据传输通道加密。（全部满足得4分）
44				**适用性：**1.核查是否已有效对数据传输通道实施加密保护；（全部满足得2分）2.核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
45				**安全性：**核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
46		数据血缘关系技术（AIT_2-AS_{16}）	3	**功能性：**检查该技术产品是否具有追踪记录数据间的血缘关系、建立数据资产全景视图等功能。（全部满足得4分）
47				**适用性：**1.核查是否已有效追踪记录数据间血缘关系，并准确地进行视图展示。（全部满足得2分）2.核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
48				**安全性：**核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
49		数据备份和恢复技术(AIT_2-AS_{17})	6	**功能性：**检查该技术产品是否具备自动化数据备份、检测备份数据完整性、数据恢复等功能。（全部满足得4分）
50				**适用性：**1. 核查该技术产品在数据遭受破坏时，数据备份和恢复机制是否有效恢复。（全部满足得2分）2.核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
51				**安全性：**核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
52		数据防泄漏技术（AIT_2-AS_{18}）	7	**功能性：**检查该技术产品是否具备数据防泄漏功能。（全部满足得4分）
53				**适用性：**1.核查该技术产品是否有效实现了数据流转过程的防泄漏。（全部满足得2分）2.核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）

表A.1　公共数据安全体系评估指标定义示例（续）

序号	评估项(AIT)	评估子项（AS）	评估权重	赋分规则
54	技术防护子体系（AIT_2）	数据防泄漏技术（AIT_2-AS_{18}）	7	**安全性：**核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
55		销毁数据识别技术（AIT_2-AS_{19}）	6	**功能性：**检查该技术产品是否具备符合多种销毁场景的数据的识别等功能。（全部满足得4分）
56				**适用性：**1. 核查该技术产品是否可有效识别并销毁符合数据销毁场景的数据。（全部满足得2分）2. 核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
57				**安全性：**核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
58		数据销毁技术（AIT_2-AS_{20}）	6	**功能性：**检查该技术产品是否具备符合多种销毁场景的数据的识别等功能。（全部满足得4分）
59				**适用性：**1. 核查该技术产品是否可有效识别并销毁符合数据销毁场景的数据。（全部满足得2分）2. 核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
60				**安全性：**核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
61		访问权限管理技术（AIT_2-AS_{21}）	8	**功能性：**检查该技术产品是否具备公共数据访问权限集中认证、统一访问入口、细粒度的访问控制等功能，与数据脱敏相关技术产品联动。（全部满足得4分）
62				**适用性：**1. 核查该技术产品是否有效支撑该组织和角色职能需求，实现公共数据访问用户的统一身份认证和访问控制。（全部满足得2分）2.核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
63				**安全性：**核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
64		数据共享和开放安全技术(AIT_2-AS_{22})	7	**功能性：**检查该技术产品是否具备访问控制、数据脱敏、接口实时数据安全监测与异常告警、据追踪溯源等功能。（全部满足得4分）
65				**适用性：**1.核查该技术产品是否可有效支撑数据共享和开放安全。（全部满足得2分）2.核查该技术产品性能是否满足该组织业务高峰期需求等。（全部满足得1分）
66				**安全性：**核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）

表A.1　公共数据安全体系评估指标定义示例（续）

序号	评估项(AIT)	评估子项（AS）	评估权重	赋分规则
67	技术防护子体系（AIT_2）	安全监测与预警技术(AIT_2-AS_{23})	7	**功能性：**检查该技术产品是否具备可配置的量化指标，是否全量接入重要系统日志，并具备支撑威胁发现、识别、理解分析、风险预警和提供处置建议等功能。（全部满足得4分）
68				**适用性：**1.核查该技术产品是否有效发现该组织数据安全风险，支撑数据安全体系建设规划。（全部满足得2分）2.核查该技术产品性能是否满足该组织高峰期业务需求等。（全部满足得1分）
69				**安全性：**核查该技术产品本身是否存在安全漏洞、配置错误、业务逻辑错误等。（全部满足得3分）
70	运行管理子体系（AIT_3）	数据安全团队(AIT_3-AS_{24})	6	**完备性：**检查是否设置了公共数据安全管理团队，并明确团队的各方的职责分工。检查是否设置了机构主要负责人为公共数据安全管理第一责任人、公共数据安全管理负责人及其工作职责。（全部满足得4分）
71				**专业性：**查验公共数据安全管理负责人是否具备数据安全专业知识和履职能力、是否接受安全技能培训和考核、是否具有必备的人力支持和技术支持；查验该团队成员专业人员安全技术能力及安全专业证书覆盖程度，接受数据安全防护技能及法规培训记录等，确保可胜任职责范围的工作。（全部满足得3分）
72				**可靠性：**查验安全管理负责人的个人自述、履历等情况；查验该团队成员的个人自述、履历等情况，确保有良好职业操守，无不良记录。（全部满足得3分）
73		数据分类分级管理机制(AIT_3-AS_{25})	6	**完整性：**查验该工作机制是否与数据资源目录机制协同、是否建立维护了数据资产全景视图、是否实现分类分级闭环工作机制。（全部满足得3分）
74				**符合性：**查验分类分级工作实施、数据资源目录同步、分级结果反馈、分类分级机制优化等工作过程文件和记录。（全部满足得3分）
75				**有效性：**检查分类分级工作结果文件和记录。（全部满足得4分）
76		数据访问权限管理机制(AIT_3-AS_{26})	8	**完整性：**查验该工作机制是否包括公共数据访问权限的分配、开通、使用、变更、重置、注销等的申请审批、实施、定期核查、清单维护等。（全部满足得3分）
77				**符合性：**查验公共数据访问账号权限管理工作过程文件和记录。（全部满足得3分）
78				**有效性：**检查公共数据访问账号权限管理工作结果文件和记录。（全部满足得4分）

表A.1　公共数据安全体系评估指标定义示例（续）

序号	评估项(AIT)	评估子项（AS）	评估权重	赋分规则
79	运行管理子体系（AIT_3）	数据共享和开放安全管理(AIT_3-AS_{27})	7	**完整性：**查验该工作机制是否包括公共数据共享和开放的申请审批，接口上线前和上线后的安全检查、敏感数据实时监测告警处置等。（全部满足得3分）
80				**符合性：**查验公共数据共享和开放安全管理工作过程文件和记录。（全部满足得3分）
81				**有效性：**检查公共数据共享和开放安全管理工作结果文件和记录。（全部满足得4分）
82		安全日志审计机制(AIT_3-AS_{28})	7	**完整性：**查验该工作机制是否包括违规行为告警的核实、分析、处置和整改等环节。（全部满足得3分，一项不足扣1分）
83				**符合性：**查验安全日志审计工作过程文件和记录。（全部满足得3分）
84				**有效性：**检查安全日志审计工作的结果文件。（全部满足得4分）
85		安全监督检查机制(AIT_3-AS_{29})	7	**完整性：**查验该工作机制是否包括安全监督检查工作实施、工作总结，问题整改、整改效果验证等环节。（全部满足得3分）。
86				**符合性：**查验安全监督检查工作过程文件和记录。（全部满足得3分）
87				**有效性：**检查安全监督检查工作结果文件和记录。（全部满足得4分）
88		安全事件应急响应机制(AIT_3-AS_{30})	8	**完整性：**查验该工作机制是否包括应急演练规划、实施、总结以及应急演练报告编制、应急预案优化等环节。
89				**符合性：**查验应急演练规划、实施、总结以及应急演练报告编制、应急预案优化等工作过程文件和记录。
90				**有效性：**检查应急演练规划、实施、总结以及应急演练报告编制、应急预案优化等工作结果文件和记录；检查安全事件发生时，应急响应工作记录和结果文件。
91		安全培训机制(AIT_3-AS_{31})	5	**完整性：**查验该工作机制是否包括培训计划制定、工作实施、效果考核、计划优化调整等环节。（全部满足得4分）
92				**符合性：**查验培训计划制定、工作实施、效果考核、计划优化调整等工作过程文件和记录。（全部满足得3分）
93				**有效性：**检查培训计划制定、工作实施、效果考核、计划优化调整等工作结果文件和记录。（全部满足得3分）

附 录 B
（资料性）
常用评估方式示例

B.1 评估方式选取

评估团队可根据评估对象及评估项的实际情况，选取合适的评估方式。

B.2 常用评估方式

B.2.1 资料查阅

评估人员查阅评估对象相关文件资料，包括但不限于项目数据安全方面的政策文件、管理制度、工作流程以及工作中的相关记录文件，用以评估公共数据安全体系是否符合标准定义的一种方法。通常在评估初期使用该方式。评估对象需要事先准备完整的文件资料以供评估人员查阅。

B.2.2 人员访谈

评估人员通过调研、访谈等形式，收集整理相关材料，评估公共数据安全体系是否有效，并发现问题，寻找整改方案的一种评估方式。通常在评估过程中深入组织实地调研时使用，组织需要安排熟悉数据流转过程，承载数据的应用、系统、网络情况，公共数据安全体系建设及运行情况的人员参加访谈。

B.2.3 问卷调查

评估人员有目的、有计划、有系统地以书面的形式提出问题的方式搜集资料，以搜集评估对象相关的现实状况或历史状况的材料进行整理、统计、分析的一种评估方式。通常在评估初期评估人员分发问卷给评估对象相关人员，组织需要安排熟悉数据流转过程，承载数据的应用、系统、网络情况，公共数据安全体系建设及运行情况的人员填写问卷。

B.2.4 功能演示

评估人员查看公共数据安全相关应用、系统等，包括功能页面、功能实现效果等，以评估公共数据安全体系是否有效的一种方法。通常在评估过程中深入调研时使用，组织安排相关人员进行现场或远程的方式演示。评估人员根据演示情况进行评估。

B.2.5 技术检测

评估人员通过人工检查、实际测试、工具扫描、应用分析、硬件检测、攻防演练或渗透测试等方式检测承载公共数据的应用、系统、网络以及相关安全系统，以评估公共数据安全体系是否有效的一种方法。通常是评估人员针对公共数据生命周期涉及的相关技术指标进行验证时使用。评估人员需要事先准备验证工具、与组织约定好评估时间，避免影响业务系统的正常运行。

附 录 C
（资料性）
计算方法示例

C.1 评估团队可根据评估指标得分计算评估子项分值,对应附录 A 的评估指标设计,可采用下文计算方法。评估子项分值等于各评估指标得分之和。评估子项分值计算公式为：

$$AS_n = X_n + Y_n + Z_n \quad \text{(C.1)}$$

式中的变量符号说明见表C.1：

表 C.1 变量符号说明表

AS_n	n取值范围	X_n	Y_n	Z_n
评估子项分值	[1,9]	全面性指标得分	可执行性指标得分	动态更新性指标得分
	[10,23]	功能性指标得分	适用性指标得分	安全性指标得分
	24	完备性指标得分	专业性指标得分	可靠性指标得分
	[25,31]	完整性指标得分	符合性指标(COMP)得分	有效性指标(E)得分

C.2 根据评估子项分值，可分别计算每个子体系评估项分值，子体系评估项分值等于该类别中各评估子项分值与其评估权重的乘积之和：

a) 制度规范子体系的评估项分值计算公式如下：

$$AIT_1 = \frac{\sum_{n=1}^{n=9} AS_n * R_{\mathrm{AS}n}}{\sum_{n=1}^{n=9} AS_{\mathrm{full}n} * R_{\mathrm{AS}n}} * 100 \quad \text{(C.2)}$$

式中：

AIT_1——制度规范子体系评估项分值；

AS_n ——评估子项分值;

R_{AS} ——评估子项权重值；

AS_{full}——评估子项满分分值；

n ——第n个评估子项。

b) 技术防护子体系的评估项分值计算公式如下：

$$AIT_2 = \frac{\sum_{n=23}^{n=10} AS_n * R_{\mathrm{AS}n}}{\sum_{n=23}^{n=10} AS_{\mathrm{full}n} * R_{\mathrm{AS}n}} * 100 \quad \text{(C.3)}$$

式中：

AIT_2——技术防护子体系评估项分值；

AS_n ——评估子项分值;

R_{AS} ——评估子项权重值；

AS_{full}——评估子项满分分值；

n ——第n个评估子项。

c) 运行管理子体系的评估项分值计算公式如下：

$$AIT_3 = \frac{\sum_{n=31}^{n=24} AS_n * R_{\mathrm{AS}n}}{\sum_{n=31}^{n=24} AS_{\mathrm{full}n} * R_{\mathrm{AS}n}} * 100 \quad \text{(C.4)}$$

式中：

AIT_3——运行管理子体系评估项分值；

AS_n——评估子项分值；

R_{NS}——评估子项权重值；

AS_{Full}——评估子项满分分值；

n——第n个评估子项。

C.3 根据评估子项分值，计算公共数据安全体系三个子体系评估项总分值，总分值计算公式如下：

$$SUM = AIT_1 + AIT_2 + AIT_3 \quad \text{(C.5)}$$

式中：

SUM——最终总分值；

AIT_1——制度规范子体系评估项分值；

AIT_2——技术防护子体系评估项分值；

AIT_3——*运行管理子体系评估项分值*。

附 录 D
（资料性）
公共数据安全体系评估案例

D.1 确定评估范围

某地公共数据管理机构依据本标准，对本机构公共数据安全体系进行整体评估，评估对象为本机构公共数据平台，涉及部门包括本机构公共数据安全管理部门、公共数据平台运维部门、公共数据相关基础设施（政务云、网络、终端等）运维部门以及公共数据平台应用部门等。

D.2 组建评估团队

由公共数据主管部门牵头，联合本机构公共数据安全管理部门、公共数据平台运维部门、相关基础设施（政务云、网络、终端等）运维部门以及重点的公共数据平台应用部门等相关人员组成评估团队。

D.3 制定评估方案

评估团队根据评估对象实际情况，确定了评估场地、评估时间。选取了全部的评估项和评估子项，参考采用附录B的评估权重和赋分规则，选择了资料查询、人员访谈、问卷调查、功能演示和技术检测等评估方式，形成书面评估方案。

D.4 实施评估

评估团队整理并记录评估佐证材料，通过不同的评估方式，初步研判各评估指标得分。得分情况详见表D.1。

表 D.1 评估指标计分表

评估项	评估子项	评估方式	评估维度	打分结果
制度规范子体系评估项（AIT_1）	数据分类分级管理制度（AIT_1-AS_1）	资料查阅 人员访谈	全面性	5
			可执行性	3
			动态更新性	2
	数据访问权限管理制度（AIT_1-AS_2）	资料查阅 人员访谈	全面性	5
			可执行性	3
			动态更新性	2
	数据脱敏管理制度（AIT_1-AS_3）	资料查阅 人员访谈	全面性	5
			可执行性	2
			动态更新性	2
	数据共享和开放安全管理制度（AIT_1-AS_4）	资料查阅 人员访谈	全面性	5
			可执行性	3
			动态更新性	1
	数据安全销毁管理制度（AIT_1-AS_5）	资料查阅 人员访谈	全面性	5
			可执行性	2
			动态更新性	1

表D.1　评估指标计分表（续）

评估项	评估子项	评估方式	评估维度	打分结果
制度规范子体系评估项（AIT_1）	供应方安全管理（AIT_1-AS_6）	资料查阅 人员访谈	全面性	5
			可执行性	3
			动态更新性	2
	安全监督检查制度（AIT_1-AS_7）	资料查阅 人员访谈	全面性	5
			可执行性	3
			动态更新性	2
	安全日志审计制度（AIT_1-AS_8）	资料查阅 人员访谈	全面性	5
			可执行性	3
			动态更新性	2
	安全事件管理与应急响应制度（AIT_1-AS_9）	资料查阅 人员访谈	全面性	5
			可执行性	3
			动态更新性	2
技术防护子体系（AIT_2）	数据源统一鉴别技术（AIT_2-AS_{10}）	功能演示 技术检测 人员访谈	功能性	4
			适用性	2
			安全性	2
	敏感数据识别技术（AIT_2-AS_{11}）	功能演示 技术检测 人员访谈	功能性	3
			适用性	3
			安全性	3
	数据分类分级标识技术（AIT_2-AS_{12}）	功能演示 技术检测 人员访谈	功能性	4
			适用性	3
			安全性	3
	数据脱敏技术（AIT_2-AS_{13}）	功能演示 技术检测 人员访谈	功能性	4
			适用性	3
			安全性	3
	数据加密技术（AIT_2-AS_{14}）	功能演示 技术检测 人员访谈	功能性	4
			适用性	2
			安全性	3
	传输通道加密技术（AIT_2-AS_{15}）	功能演示 技术检测 人员访谈	功能性	4
			适用性	3
			安全性	3
	数据血缘关系技术（AIT_2-AS_{16}）	功能演示 技术检测 人员访谈	功能性	3
			适用性	3
			安全性	3
	数据备份和恢复技术（AIT_2-AS_{17}）	功能演示 技术检测 人员访谈	功能性	4
			适用性	2
			安全性	1

表D.1　评估指标计分表（续）

评估项	评估子项	评估方式	评估维度	打分结果
技术防护子体系（AIT_2）	数据防泄漏技术(AIT_2-AS_{18})	功能演示	功能性	4
		技术检测	适用性	3
		人员访谈	安全性	3
	销毁数据识别技术(AIT_2-AS_{19})	功能演示	功能性	3
		技术检测	适用性	2
		人员访谈	安全性	3
	数据销毁技术(AIT_2-AS_{20})	功能演示	功能性	4
		技术检测	适用性	2
		人员访谈	安全性	3
	访问权限管理技术(AIT_2-AS_{21})	功能演示	功能性	3
		技术检测	适用性	3
		人员访谈	安全性	3
	数据共享和开放安全技术(AIT_2-AS_{22})	功能演示	功能性	4
		技术检测	适用性	2
		人员访谈	安全性	1
	安全监测与预警技术(AIT_2-AS_{23})	功能演示	功能性	4
		技术检测	适用性	3
		人员访谈	安全性	3
运行管理子体系（AIT_3）	数据安全团队(AIT_3-AS_{24})	资料查阅	完备性	3
		人员访谈	专业性	3
		问卷调查	可靠性	3
	数据分类分级管理机制(AIT_3-AS_{25})	资料查阅	完整性	3
		功能演示	符合性	3
		人员访谈	有效性	4
	数据访问权限管理机制(AIT_3-AS_{26})	资料查阅	完整性	2
		功能演示	符合性	3
		人员访谈	有效性	2
	数据共享和开放安全管理(AIT_3-AS_{27})	资料查阅	完整性	2
		功能演示	符合性	3
		人员访谈	有效性	3
	安全日志审计机制(AIT_3-AS_{28})	资料查阅	完整性	3
		功能演示	符合性	3
		人员访谈	有效性	3
	安全监督检查机制(AIT_3-AS_{29})	资料查阅	完整性	3
		功能演示	符合性	3
		人员访谈	有效性	4

表D.1　评估指标计分表（续）

评估项	评估子项	评估方式	评估维度	打分结果
运行管理子体系（AIT_3）	安全事件应急响应机制(AIT_3-AS_{30})	资料查阅 功能演示 人员访谈	完整性	2
			符合性	3
			有效性	2
	安全培训机制(AIT_3-AS_{31})	资料查阅 功能演示 人员访谈	完整性	2
			符合性	3
			有效性	3

评估团队召开复评会议，根据评估过程记录及评估证明材料，最终研判核准各评估指标得分，核准得分后，得出评估结果。

按附录C的式（C.1）计算评估子项分值，各评估子项权重值和分值见表D.2。

表 D.2　评估结果表

评估项	评估子项	评估权重值	评估子项分值（复评）
制度规范子体系评估项（AIT_1）	数据分类分级管理制度（AIT_1-AS_1）	6	8
	数据访问权限管理制度（AIT_1-AS_2）	7	10
	数据脱敏管理制度（AIT_1-AS_3）	7	8
	数据共享和开放安全管理制度（AIT_1-AS_4）	7	9
	数据安全销毁管理制度（AIT_1-AS_5）	5	8
	供应方安全管理（AIT_1-AS_6）	8	10
	安全监督检查制度（AIT_1-AS_7）	5	10
	安全日志审计制度（AIT_1-AS_8）	7	8
	安全事件管理与应急响应制度（AIT_1-AS_9）	8	10
技术防护子体系评估项（AIT_2）	数据源统一鉴别技术(AIT_2-AS_{10})	4	8
	敏感数据识别技术(AIT_2-AS_{11})	8	8
	数据分类分级标识技术(AIT_2-AS_{12})	8	9
	数据脱敏技术（AIT_2-AS_{13}）	8	8
	数据加密技术 (AIT_2-AS_{14})	5	8
	传输通道加密技术(AIT_2-AS_{15})	6	9
	数据血缘关系技术(AIT_2-AS_{16})	3	8
	数据备份和恢复技术(AIT_2-AS_{17})	6	7
	数据防泄漏技术(AIT_2-AS_{18})	7	8
	销毁数据识别技术(AIT_2-AS_{19})	6	8
	数据销毁技术(AIT_2-AS_{20})	6	9
	访问权限管理技术(AIT_2-AS_{21})	8	9
	数据共享和开放安全技术(AIT_2-AS_{22})	7	7
	安全监测与预警技术(AIT_2-AS_{23})	7	9

表D.2 评估结果表（续）

评估项	评估子项	评估权重值	评估子项分值（复评）
运行管理子体系评估项（AIT_3）	数据安全团队(AIT_3-AS_{25})	6	9
	数据分类分级管理机制(AIT_3-AS_{26})	6	9
	数据访问权限管理机制(AIT_3-AS_{27})	8	7
	数据共享和开放安全管理(AIT_3-AS_{28})	7	8
	安全日志审计机制(AIT_3-AS_{29})	7	9
	安全监督检查机制(AIT_3-AS_{30})	7	10
	安全事件应急响应机制(AIT_3-AS_{31})	8	7
	安全培训机制(AIT_3-AS_{32})	5	8

根据评估子项分值和评估权重，按式（C.2）、式（C.3）和式（C.4）计算评估项分值，计算得出制度规范子体系评估项加权平均得分为90分，技术防护子体系评估项得分为83分，运行管理子体系评估项得分为83分。

根据所有评估子项分值，按式（C.5）计算最终总分值。计算得出最终分值为85分。

D.5 报告编制

从评估得分可以判断该单位基本建立形成公共数据安全体系。

评估团队详细分析了评估指标分值，发现评估对象在制度规范、技术防护和运行管理三个方面发展较为平衡，制度规范子体系的动态更新性有待提高，技术防护子体系的适用性有待进一步加强，例如数据源统一鉴别、数据共享和开放安全技术等。

评估团队针对公共数据安全体系建设的薄弱环节，提出相应的整改建议。例如，针对制度规范子体系的动态更新性薄弱的问题，建议指定专人持续跟踪外部环境、政策变化，及时调研机构实际情况，建立制度规范子体系更新工作机制;针对数据共享和开放安全技术产品缺乏有效的接口安全风险探测手段的问题，建议通过流量探针、服务探针等方式，及时监测并处置接口安全风险。

最终，评估团队形成了评估报告，帮助该机构持续提升公共数据安全体系化水平和防护能力。

参 考 文 献

[1] 浙江省公共数据安全管理总则
[2] 浙江省公共数据访问权限管理规范
[3] 浙江省公共数据安全脱敏技术规范
[4] 浙江省公共数据安全销毁技术规范
[5] 浙江省公共数据安全日志审计规范
[6] 浙江省一体化智能化公共数据平台省级数据回流工作细则